



BALABIT
CONTEXTUAL SECURITY INTELLIGENCE

Tesztlaborok gombnyomásra

Höltzl Péter, senior trainer
HOUG konferencia, Április 2018

Miről lesz szó?

- Mitől lesz jó egy training?
- Milyen kihívások vannak egy labor környezet felépítésében
- Hogyan építettük fel a Balabit labor környezetét?

A Balabit bemutatása

- 18 éve az IT Security-ben
- 1300+ ügyfél
- 100+ Partner
- 25+ Fortune 100-as ügyfél
- Irodák: Budapest, New York, London, Párizs, München, Moszkva
- 2018-tól a Quest/One Identity része

Termékeink

- Termékek:
 - Zorp (2015-ig)
 - PSM (ex SCB) (2006 óta)
 - syslog-ng OSE és PE (1999 óta)
 - syslog-ng Store Box (2009 óta)

Technical trainingek

- Instructor-led, classroom based
- On-site training
- Termékek szerint:
 - PSM Technical Training
 - syslog-ng Technical Training
 - syslog-ng Store Box Technical Training
 - Troubleshooting Technical Training

Milyen egy jó training?

- Elmélet, Gyakorlat (Labor) megfelelő arányban
- Prezentáció
- Feladatok és Exercise Book (sokszor nyomtatva)
- Mindenkinek teljesen ugyanaz a környezet

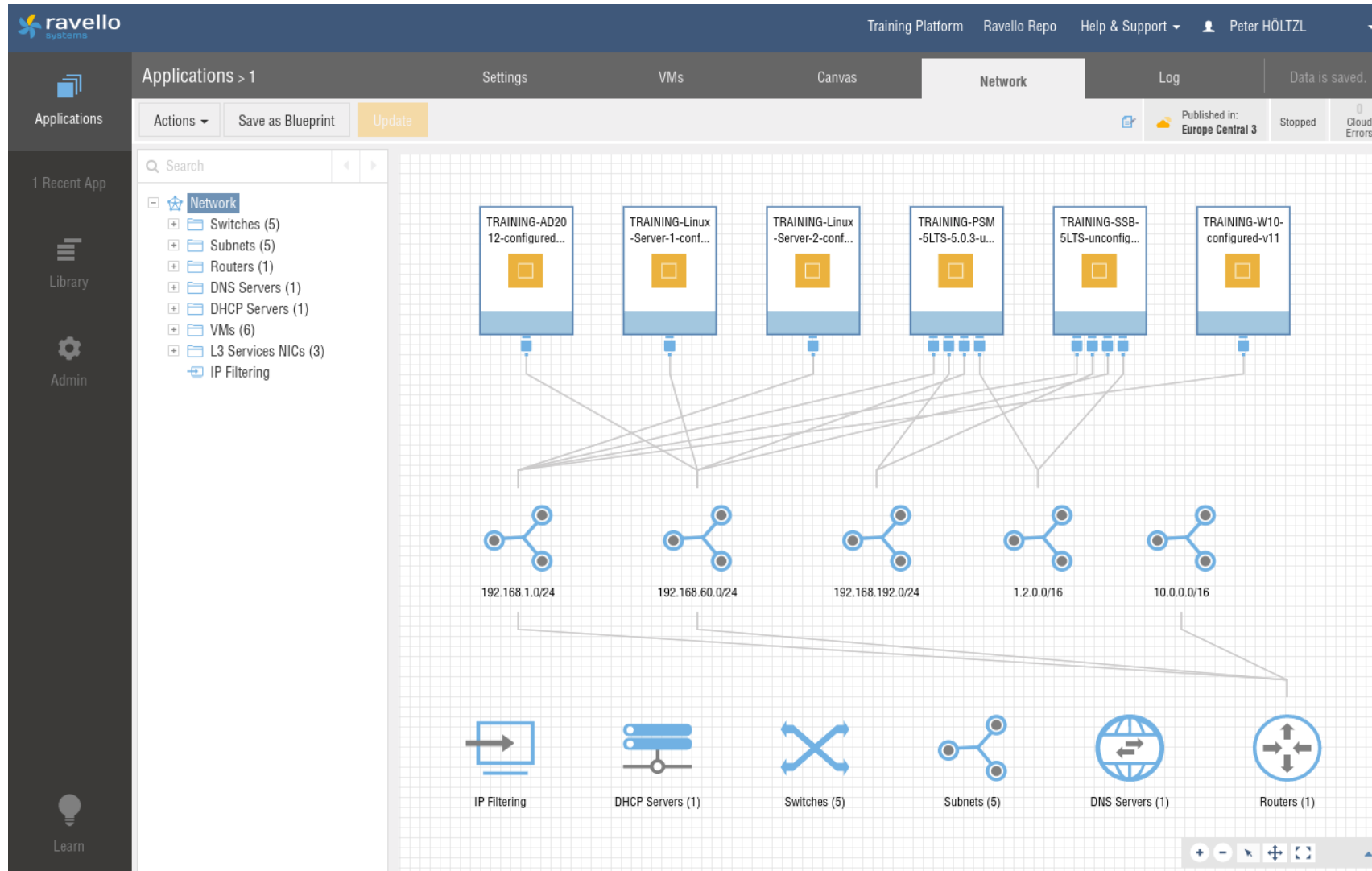
Milyen problémákba ütköztünk

- Saját hosting
 - Erőforrás igény
 - Üzemeltetés, karbantartási igény, frissítések
 - Elérés, latency
- Hallgatói hosting
 - Mindenkinek más a rendszere
 - A saját gépemen nincs virtualizáció engedélyezve
 - A gépem lassú, kevés az erőforrás (következő slide)
 - Nem tudom a BIOS jelszót!

Erőforrás igény

- PSM: 5 host, 6 core, 24GB RAM, 100Gb Storage, 2 network (~1.2USD/h)
- syslog-ng/SSB: 4 host, 5 core, 16GB RAM, 60GB storage, 1 network (~0.8USD/h)
- Troubleshooting: 6 host, 7 core, 28GB RAM, 100Gb Storage, 2 network (~1.4USD/h)

Topológia



Kellett egy megoldás, ami(t)...

- Nem mi üzemeltetünk
- Template alapú (blueprint)
- Mindenhol elérhető
- Könnyen elérhető (RDP)
- Minden hallgatónál egyforma
- A hallgatókat elkülöníti
- Automatizált
- Illeszthető a rendszerünkhöz (van API)
- Megy a mi termékünk (nem XEN álló): HVX

Itt jött a képbe a Ravello

- Importált image-ek (VM)
 - Ravello import tool (linux is!)
- Blueprint: template környezet
- App: A blueprint materializálása
- Ephemeral Access: Időzített access a Ravello account nélküli felhasználóknak
- Elastic IP
- Port forward (külső hozzáférés)

Mit lát a hallgató?

Troubleshooting Balabit Products

6 VMs are stopped All VMs: [Start](#) / [Stop](#) [Help](#)

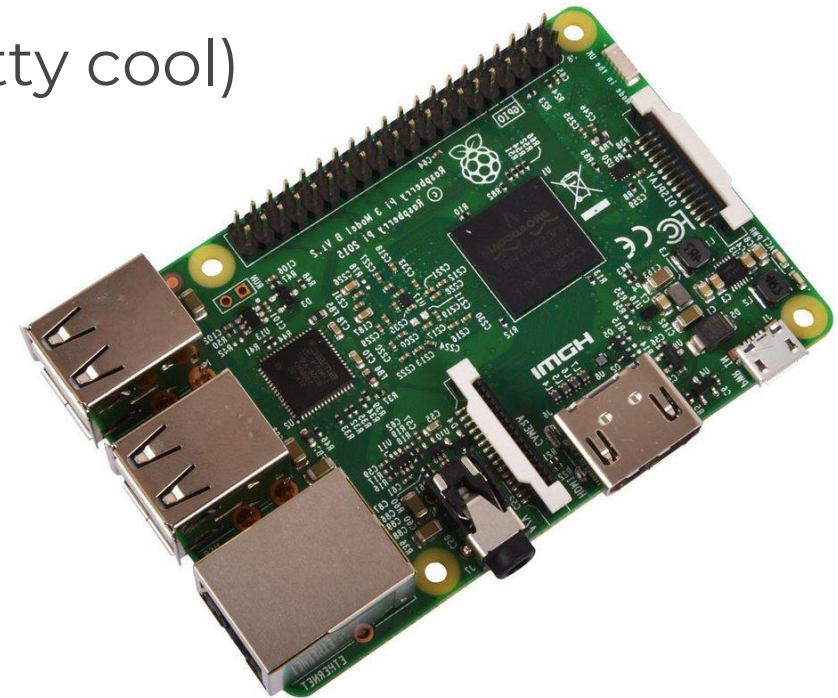
<p>Stopped</p> <p>TRAINING-AD2012-configured-...</p> <p>SERVICES No services</p> <p>CONSOLE</p> <p>ACTIONS ▶ ■ ↺ 🔌</p>	<p>Stopped</p> <p>TRAINING-Linux-Server-2-confi...</p> <p>SERVICES ssh@443</p> <p>CONSOLE</p> <p>ACTIONS ▶ ■ ↺ 🔌</p>	<p>Stopped</p> <p>TRAINING-PSM-5LTS-5.0.3-unc...</p> <p>SERVICES No services</p> <p>CONSOLE</p> <p>INFO MORE ▾ Your freshly installed SCB as Balalabit ships the product. It requires initialization. To start it, just op...</p> <p>ACTIONS ▶ ■ ↺ 🔌</p>	<p>Stopped</p> <p>TRAINING-SSB-5LTS-unconfigur...</p> <p>SERVICES No services</p> <p>CONSOLE</p> <p>ACTIONS ▶ ■ ↺ 🔌</p>
<p>Stopped</p> <p>TRAINING-Linux-Server-1-confi...</p> <p>SERVICES No services</p> <p>CONSOLE</p> <p>INFO TRAINING-Linux-1</p>	<p>Stopped</p> <p>TRAINING-W10-configured-v11</p> <p>SERVICES rdp@443 / rdp@3389</p> <p>CONSOLE</p>		

Integráció

- Ravello API + MyBalabit integráció
- App legyártása Blueprint ID-ból
- Ephemeral Access legyártása → Link a mybalabit-en
- Training után Ephemeral törlése
- Training után App törlése

Hozzáférés

- Console (VNC over HTTPS)
- PortForward (Windows 10 JumpHost + RDP)
- Balabit training room:
 - Raspberry Pi + Ubuntu MATE (olcsó és pretty cool)



Mit lát a felhasználó?

The image shows a Ravello Systems virtual machine environment. The top bar displays the application name 'Troubleshooting Balabit Products', the VM name 'TRAINING-W10-configured-v11', the DNS 'trainingw10configu-1-yldyu0qi.srv.ravcloud.com', and the internal IP '192.168.1.2'. The main display area is split into two parts:

- Top Right:** A graphical login screen for 'balabit'. It features a background image of a natural rock archway over a beach. A circular icon with a person silhouette is centered, with the word 'balabit' below it. At the bottom right, there are icons for language (ENG/US), a monitor, a refresh button, and a power button.
- Bottom Left:** A terminal window showing boot logs and instructions. The logs indicate a fatal error during core firmware initialization and a subsequent restart of the syslog-ng service. The instructions state that configuration is done via the web interface at `https://192.168.1.1/` and prompt for 'scb1 login:'.

Nice features

- Share blueprint (bárkivel, akinek van oracle access-e)
- Cost alert
- Buckets
- Scheduling

Ami jól jönne

- Okosabb port forward (PAT)
- 3D támogatás (OpenGL)
- App relokáció
- Training platform API támogatás

Q&A

Höltzl Péter

peter.holtzl@balabit.com